Google Scholar BETA

Web Images Video News Maps more »

signature "braid groups" Search

Advanced Scholar Search
Scholar Preferences
Scholar Help

Scholar **All articles** - **Recent articles** Results **21** - **30** of about **369** for **signature "braid groups"**. (0.

All Results
V JONES
P FREYD
D YETTER
J HOSTE
W LICKORISH

[PDF] Quantum SU (2) faithfully detects mapping class groups modulo center - all 70 versions »
MH Freedman, K Walker, Z Wang - Geometry & Topology, 2002 - emis.ams.org
... **braid groups** B n , sometimes called the generic q{analog{SU(2){representation, is not known to ... by interpreting L as a surgery diagram, and on the **signature** of L ...
Cited by 8 - Related Articles - View as HTML - Web Search

[PDF] Provably-Secure Identification Scheme based on Braid Group - all 2 versions »
Z Kim, K Kim - SCIS 2004 - caislab.icu.ac.kr
... Shamir [4] and Shoup [13], the distinction between identification and **signature** schemes is ... 2.1 **Braid Groups** A braid is obtained by laying down a number of par ...
Cited by 4 - Related Articles - View as HTML - Web Search

Random Subgroups of **Braid Groups**: An Approach to Cryptanalysis of a Braid Group Based Cryptographic ...
A Myasnikov, V Shpilrain, A Ushakov - 2006 - Springer
... 100 Page 4. Random Subgroups of **Braid Groups** 305 and ... w|. Algorithm 1. (Minimization of braids) **Signature**. w = Shorten(w). Input. A ...
Cited by 3 - Related Articles - Web Search

New Digital **Signature** Scheme in Gaussian Monoid - all 2 versions »
E SAKALAUSKAS - Informatica, 2004 - IOS Press
... It is a pure **signature** scheme based on group theory mechanism (on group ... One known
solution for **Braid groups** is an application of left-weighted canonical (normal ...
Cited by 3 - Related Articles - Web Search

[PDF] Undeniable **Signature** Schemes Using **Braid Groups** - all 4 versions »
T Thomas, AK Lal - Arxiv preprint cs.CR/0601049, 2006 - arxiv.org
... Undeniable **Signature** Schemes Using **Braid Groups** May 18, 2006 ... undeniable **signature**
schemes based on **braid groups** or even in any nonabelian group setting. ...
Cited by 1 - Related Articles - View as HTML - Web Search

[PDF] Authentication Schemes Using **Braid Groups** - all 3 versions »
S Lal, A Chaturvedi - Arxiv preprint cs.CR/0507066, 2005 - arxiv.org
... cryptosystem using **braid groups**, Advances in Cryptology, Proceeding of Crypto - ... 5. KH.Ko, DH.Choi, MS.Cho, and JW.Lee, New **signature** scheme using conjugacy ...
Cited by 3 - Related Articles - View as HTML - Web Search

[PS] Chern Classes of Fibered Products of Surfaces - all 46 versions »
M Teicher - **Signature** - emis.ams.org
... topological invariants. These Chern classes satisfy: c 2 1 ; c 2 0 5 c 2 1
c 2 36 **Signature** = = 1 3 (c 2 1 2 c 2) The famous Bogomolov ...
Cited by 5 - Related Articles - View as HTML - Web Search

Google Scholar BETA

Web Images Video News Maps more »

"digital signature" "braid group conjugacy" Search

Advanced Scholar Search
Scholar Preferences
Scholar Help

There were no results in your selected language(s). Showing worldwide web results for **"digital signature" "braid group conjugacy"**.

Scholar

Results **1** - **2** of **2** for **"digital signature" "braid group conjugacy"**. (**0.28** seconds)

All Results
K Ko
S Lee
J Cheon
J Han
J Kang

Tip: Try removing quotes from your search to get more results.

New Public-Key Cryptosystem Using Braid Groups - all 12 versions »
KH Ko, SJ Lee, JH Cheon, JW Han, J Kang, C Park, K ... - Advances in Cryptology-Crypto 2000: 20th Annual ..., 2000 - books.google.com
... Key words: public key cryptosystem, **braid group**, **conjugacy** problem, key exchange, hard problem, non ... But we don't have a **digital signature** scheme based on the ...
Cited by 126 - Related Articles - Web Search

Digital signature method based on braid groups conjugacy and verify method thereof
K Code, Y Ding, J Chen, Z Peng, VP Images, P Class ... - freepatentsonline.com
The present invention discloses a **digital signature** scheme based on **braid group conjugacy** problem and a verifying method thereof, wherein the signatory S ...
Cached - Web Search

"digital signature" "braid group conj Search

Google Home - About Google - About Google Scholar

Google Scholar BETA

Web Images Video News Maps more »

cryptosystem "Braid group" Search

Advanced Scholar Search
Scholar Preferences
Scholar Help

There were no results in your selected language(s). Showing worldwide web results for **cryptosystem "Braid group"**.

Scholar **All articles** - **Recent articles** Results **1** - **10** of about **179** for **cryptosystem "Braid group"**. (

All Results
K Ko
I Anshel
J Cheon
S Lee
J Han

New Public-Key **Cryptosystem** Using Braid Groups - all 12 versions »
KH Ko, SJ Lee, JH Cheon, JW Han, J Kang, C Park, K ... - Advances in Cryptology-Crypto 2000: 20th Annual ..., 2000 - books.google.com
... widely used **cryptosystems** based on number theory, but there are some similarities in design. Key words: public key **cryptosystem**, **braid group**, conjugacy problem ...
Cited by 126 - Related Articles - Web Search

A Linear Algebraic Attack on the AAFG1 **Braid Group Cryptosystem** - all 9 versions »
J Hughes - The 7th Australasian Conference on Information Security and ..., 2002 - Springer
... be hard, it may still not be suitable for a **cryptosystem**. ... 30,25,6]. Even after these **cryptosystems** failed, the ... For the **braid group** itself, little work has been ...
Cited by 26 - Related Articles - Web Search

A practical attack on some **braid group** based cryptographic primitives - all 6 versions »
D Hofheinz, R Steinwandt - Public Key Cryptography, 6th International Workshop on ..., 2003 - Springer
Page 1. A Practical Attack on Some **Braid Group** Based ... n → S n from the **braid group** B n into the symmetric group S n which maps σ i onto ...
Cited by 37 - Related Articles - Web Search

New Key Agreement Protocols in **Braid Group** Cryptography - all 4 versions »
I Anshel, M Anshel, B Fisher, D Goldfeld - Topics in Cryptology-CT-RSA2001 - Springer
New Key Agreement Protocols in **Braid Group** ... At the heart of a public key **cryptosystem** is a two-party ... The major public key **cryptosystems** in use today, and their ...
Cited by 44 - Related Articles - Web Search

Length-based conjugacy search in the **braid group** - all 6 versions »
D Garber, S Kaplan, M Teicher, B Tsaban, U Vishne - Algebraic Methods in Cryptography: Special Session on ..., 2006 - books.google.com
... A Practical Attack on Some **Braid Group** Based Cryptographic ... New Public- key **Cryptosystem**
using Braid ... of some group based **cryptosystems**, Contemporary Mathematics ...
Cited by 23 - Related Articles - Web Search - BL Direct

[PDF] Length-Based Attacks for Certain Group Based Encryption Rewriting Systems - all 19 versions »
J Hughes, A Tannenbaum - Arxiv preprint cs.CR/0306032, 2003 - arxiv.org
... is well-defined and for the **braid group** can be ... to more general types of string rewriting **cryptosystems**, and so ... In Section 5, the braid **cryptosystem** of [1] is ...
Cited by 33 - Related Articles - View as HTML - Web Search

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	7	(cryptosystem with "Braid groups")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/12/13 17:53
L2	0	"digital near signature" same "Braid groups"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/12/13 17:54
L3	0	"digital near signature" same "Braid"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/12/13 17:54
L4	0	"digital near signature" same "braid"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/12/13 17:54
L5	0	"digital near signature" same braid	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/12/13 17:54
L6	0	"digital near signature" same conjuagcy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/12/13 17:54
L7	0	"digital near signature" same conjugacy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/12/13 18:00

EAST Search History

L8	3	signature same conjugacy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/12/13 17:55
L9	42	"braid group"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/12/13 17:55
L10	4	"braid group" same (right left)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/12/13 17:56
L11	0	("2004/0120515").URPN.	USPAT	OR	ON	2007/12/13 17:58
L12	3	signature same conjugacy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/12/13 18:03
L13	51	left near subgroup	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/12/13 18:03
L14	1	(left near subgroup) and braid	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/12/13 18:40
L15	2	"20040240672"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/12/13 18:40

EAST Search History

S1	2	"20040240672"	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	ON	2007/07/12 16:39
S2	2473	(380/28)".cclas"	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	ON	2007/07/13 18:01
S3	1332	380/28.ccls.	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	ON	2007/07/12 16:39
S4	3	braid NEAR2 group near conjugacy	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	ON	2007/07/12 16:45
S5	3	("20040174278" | "20040240672" | "5241309").PN. OR ("7133523"). URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/07/12 16:42
S6	1	("2004/0240672").URPN.	USPAT	OR	ON	2007/07/12 16:43
S7	3	("20040174278" | "20040240672" | "5241309").PN. OR ("7133523"). URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/07/12 16:43
S8	126	braid NEAR2 group	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	ON	2007/07/12 16:45
S9	133	braid NEAR2 group	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/12 16:46
S10	5	braid NEAR2 group with verify$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/12 16:49

EAST Search History

S11	4	braid NEAR2 group with signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/12 16:58
S12	2	"6,493449".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/13 14:34
S13	0	ding-yong-$.in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/12 17:42
S14	8135	ding-$.in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/12 17:42
S15	52	ding-$.in. AND yong	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/12 17:44
S16	0	chen-janyong-$.in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/12 17:44
S17	8	chen-$.in. AND jianyong	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/12 17:45

EAST Search History

S18	10543	peng-$.in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/12 17:45
S19	9	peng-$.in. AND zhiwei	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/13 06:53
S21	2	"5627893".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/13 06:55
S22	4	"4405829".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/13 08:39
S23	2	"7133523".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/13 08:58
S24	224	"simple conjugacy signature scheme" OR "SCSS"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/13 09:04
S25	11528	"conjugacy signature scheme" OR "CSS"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/13 08:59

EAST Search History

S26	7	S24 WITH S25	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/13 09:00
S27	12	S24 and S25	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/13 09:00
S28	11	braid SAME key SAME message	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/13 09:05
S29	24	("4649233" | "5124117" | "5222140" | "5251258" | "5369705").PN. OR ("5729608").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/07/13 09:06
S30	1	("2002/0001382").URPN.	USPAT	OR	ON	2007/07/13 09:34
S31	0	signature with braid with verify$4	USPAT	OR	ON	2007/07/13 09:35
S32	83	signature with group with verify$4	USPAT	OR	ON	2007/07/13 09:37
S33	4	braid same key same message	USPAT	OR	ON	2007/07/13 09:38
S34	11	braid same key same message	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/13 09:41
S35	249	"ECSS"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/13 09:42
S36	2	"ECSS" with signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/13 09:42

EAST Search History

S37	432309	algorithm NEAD "BCDA"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/13 09:43
S38	1	algorithm NEAR "BCDA"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/13 12:38
S39	0	braid SAME conjuagcy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/13 12:38
S40	10	braid SAME conjugacy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/13 13:09
S41	11528	"simple conjugacy signature scheme" OR "SCSS" SAME "conjugacy signature scheme" OR "CSS"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/13 13:09
S42	7	("simple conjugacy signature scheme" OR "SCSS") SAME ("conjugacy signature scheme" OR "CSS")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/13 13:37
S43	489	"4993068"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/13 13:37

EAST Search History

S44	2	"4993068".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/13 13:41
S47	1	"10579801"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/13 14:34
S48	1	10/579801	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/13 14:35
S49	0	10/579801 and S39	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/13 17:29
S50	1	10/579801 and range	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/13 17:09
S53	2	"5850442".pn.	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	ON	2007/07/13 17:27
S54	1	10/579801 and (public NEAR key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/13 17:29

EAST Search History

S55	1	10/579801 and ((public NEAR key) SAME out NEAR band)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/13 17:30
S56	2473	(380/28)".ccls"	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	ON	2007/07/13 18:02
S57	72	(380/28-30)".ccls"	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	ON	2007/07/13 18:03
S58	9507	(380/28 OR 380/29 OR 380/30 OR 380/277 OR 713/176 OR 713/177 OR 713/188)".ccls"	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	ON	2007/07/18 13:45
S59	13566	(380/28 OR 380/29 OR 380/30 OR 380/277 OR 713/1 OR 713/176 OR 713/177 OR 713/188 OR 713/180)". ccls"	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	ON	2007/07/13 18:25
S62	1	algorithm NEAR "BCDA"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/13 18:25
S63	0	10/492894.pn.	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	ON	2007/07/18 13:42
S64	1	10/492894	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	ON	2007/07/18 13:42
S65	2	09/030935	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	ON	2007/07/18 13:43

EAST Search History

S66	10194	(380/28 OR 380/29 OR 380/30 OR 380/277 OR 713/176 OR 713/177 OR 713/188 713/176 OR 713/180 OR 713/181 OR 713/187)".ccls"	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	ON	2007/07/18 13:47
S67	1	hash$3 WITH braid$1	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	ON	2007/07/18 13:47
S68	29444	braid$1	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	ON	2007/07/18 13:47
S69	9	braid$1 AND S66	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	ON	2007/07/18 13:47